CLAIMS

1. Method of communication between a first unit (2) and a second unit (1) via a telecommunications network (R), in which the first unit comprises applications (3, 4) belonging respectively to a first family and a second family having a priori a lower degree of confidence than the first family, characterized in that each request originating from an application (4) of the second family, transmitted over the network to the second unit, is forced to include a mark associated with the second family of applications.

2. Method according to Claim 1, in which the said mark is included in each request transmitted over the network (R) and originating from an application of the second family (4).

3. Method according to Claim 1 or 2, in which the mark, included in a request transmitted over the network (R) and originating from an application (4) of the second family, is forced to include an indication of the nature and/or origin of the said application of the second family.

4. Method according to Claim 3, in which the said application (4) of the second family being signed, the mark included in the requests that originated therefrom is forced to include data relating to the certification of the signature.

5. Method according to Claim 3 or 4, in which the said application (4) of the second family having been downloaded via the network (R) from a download address, the mark included in the requests that originated therefrom is forced to include data relating to the download address of the application.

6. Method of communication between a first unit (2) and a second unit (1) via a telecommunications network (R), in which the first unit comprises applications (3, 4) belonging respectively to a first family and to a second family having a priori a lower degree of confidence than the first family, characterized in that each request originating from an application (4) of the second family, transmitted over the network to the second unit, is forced to exclude a mark associated with the first family, the said mark being included in at least some of the requests transmitted over the network and originating from applications (3) of the first family.

7. Method according to any one of the preceding claims, in which the second unit (1) examines whether the mark is present in a request received over the network (R) from the first unit (2), to assess a degree of confidence to be attached to the said request.

8. Method according to Claim 7, in which, when the mark is present in the said request, the second unit (1) also examines data included in this mark, to assess a degree of confidence to be attached to the said request.

9. Method according to Claim 8, in which the said data examined by the second unit (1) comprise data relating to the certification of a signature of the application from which the request originated.

10. Method according to Claim 8, in which the said data examined by the second unit (1) comprise data relating to a download address of the application from which the request originated.

11. Method according to any one of the preceding claims, in which the requests comprise HTTP requests,

and the mark is inserted in the headers of the HTTP requests.

12. Method according to any one of the preceding claims, in which the requirement relating to the mark is controlled by a software layer (5) belonging to a virtual machine (6) with which the first unit (2) is provided, the applications (4) of the second family being able to access the network (R) only via the virtual machine and the said software layer.

13. Method according to Claim 12, in which the virtual machine (6) is a Java virtual machine.

14. Communication terminal (2), comprising means of using a method according to any one of the preceding claims as a first unit.